Claims

WHAT IS CLAIMED IS:

1. In an initiating system, a method for establishing a group membership with a group identity information document comprising:

creating group identity information for inclusion in the group identity information document; and

generating a self-signed group identity information document comprising the group identity information, at least a first key, and a group identity information document signature signed using a second key associated with the first key in the identity information document.

2. The method of claim 1 further comprising:

sending the group-signed group identity information document to a receiving system to establish the group identity at the receiving system.

3. The method of claim 2, further comprising:

sending a group-signed membership identity information document with the group-signed group identity information document to the receiving system to establish membership of an originator of the membership identity information document in the group identity established at the receiving system.

4. The method of claim 3 further comprising:

receiving the group-signed membership identity information document from the originator;

detecting whether the group associated with the membership identity information document has been accepted; and

assigning security protocols to communications from the originator based on the group identity information if the group identity information is accepted.

5. The method of claim 3, wherein the act of sending comprises:

storing the group-signed membership identity information document in an initiating system;

retrieving the group-signed membership identity information document;

attaching the group-signed membership identity information document to the message; and

sending the message to the receiving system.

6. The method of claim 3, further comprising:

sending to the receiving system a self-signed personal identity information document of the originator of the message to establish at the receiving system identity of the originator in addition to originator's membership in the group.

7. The method of claim 6, wherein the acts of sending a self-signed personal identity information document and group-signed membership identity information document comprise;

generating the self-signed personal identity information document;

attaching the self-signed personal identity information document to the message;

retrieving the group-signed membership identity information document;

attaching the group-signed membership identity information document to the message; and

sending the message to the receiving system.

.

8. The method of claim 6 further comprising:

receiving the group-signed membership identity information document and the self-signed personal identity information document from the originator;

detecting whether the group associated with the membership identity information document is accepted and whether the person associated with the personal identity information document is accepted;

assigning first security protocols to communications from the originator if the group is accepted; and

assigning second security protocols to communications from the originator if the person is accepted.

9. In a communication system, apparatus for establishing a group identity comprising:

a group ID generate module generating a group certificate having at least a public key and a digital signature for the group; and

a send module transmitting the group certificate to establish the group identity at a receiving system.

10. The apparatus of claim 9 further comprising:

an attach module attaching a group membership certificate to a message originated by a sender;

the send module transmitting the message to the receiving system to establish the sender as a member of the group at the receiving system.

11. The apparatus of claim 10 further comprising:

a membership ID generate module generating a membership certificate having at least a public key of the sender and a digital signature for the group;

a save module, responsive to the membership ID generate module, storing the membership certificate;

a retrieve module retrieving the membership certificate from the save module and providing the membership certificate to the attach module.

12. The apparatus of claim 10 further comprising:

a receive module at the receiving system receiving the membership certificate;

an accept module at the receiving system detecting whether to accept the membership certificate.

13. The apparatus of claim 12 further comprising:

an assign module assigning a security identification to communications from the sender based on the group associated with the membership certificate if the membership certificate is accepted by the accept module.

14. The apparatus of claim 10 further comprising:

a personal ID generate module generating a personal certificate having at least a public key of the sender and a digital signature by the sender;

the send module transmitting the personal certificate to establish the sender's identity at the receiving system.

15. The apparatus of claim 14 further comprising:

a receive module at the receiving system receiving the certificates;

an accept module at the receiving system detecting if the certificates are to be accepted;

an assign module assigning a security protocol to communications from the sender based on a group identity associated with the membership certificate if the membership certificate is accepted by the accept module; and

the assign module assigning a security protocol to communications from the sender based on personal identity associated with the personal certificate if the personal certificate is accepted by the accept module.

16. A computer readable medium readable by a computing system and encoding a computer program of instructions for executing a computer process for establishing a group identity in a communications between an initiating system and a receiving system, said computer process comprising:

generating at the initiating system a group certificate having at least a group public key and a digital signature for the group signed with a group private key associated with group public key; and

sending the group certicate to the receiving system to establish the group identity at the receiving system.

17. The computer readable medium of claim 16 wherein the process further comprises:

sending a membership certificate to the receiving system to establish the originator as a member of the group at the receiving system.

18. The computer readable medium of claim 17 wherein the process further comprises:

creating the membership certificate at the initiating system, the membership certificate having at least a public key of the originator and a digital signature signed using the group private key.

19. The computer readable medium of claim 17 wherein the process further comprises

receiving the membership certificate at the receiving system; and

testing acceptance of the group identity received in the membership certificate.

20. The computer readable medium of claim 19 wherein the process further comprises

assigning a security protocol to communications from the originator based on the group identity if the membership certificate is accepted by the act of testing.

21. The computer readable medium of claim 17 wherein the process further comprises

generating a personal certificate having at least a public key of the originator and a digital signature for the originator signed by the originator with a private key associated with the public key of the originator;

sending the personal certificate to establish the personal identity of the originator at the receiving system.

22. The computer readable medium of claim 21 wherein the process further comprises accepting the identity information in the certificates received at the receiving system if the certificates have been previously accepted;

assigning a security identification to communications from the originator based on the group identity information if the membership certificate is accepted; and

assigning a security identification to communications from the originator based on the personal identity information of the originator if the personal certificate is accepted.